The bridge to possible

Cisco Network Security—Security That Is Built In Not Bolted On

Product overview

Cisco is a leader in networking and a leader in security. Who better to integrate the two domains to deliver solutions that are more effective than any solution cobbled together from different vendors?

Cisco integrates network security control points and common telemetry to help ensure an airtight level of security on your network. Through the combined footprint of both solutions, your network can automatically and effectively protect your users and assets, regardless of where across the distributed network they exist. By applying machine learning and analytics to the information generated by the network, users, devices, and applications, your network can automatically confirm policies and shut down out-of-compliance behavior. Ultimately this reduces the time to detection and expedites the remediation of threats.

Our wide range of network security solutions work hand in glove to deliver security in depth as well as complete zero-trust security frameworks. You'll get the benefits of a leading security solution that is optimized for our leading networking infrastructure.

Benefits

Cisco® networking and security solutions combine to deliver the best of both worlds. With Cisco, you can:

- **Leverage integrated network security control points** in network infrastructure to increase the effectiveness of your security
- **Use common telemetry** for both networking and security to minimize operations complexity
- **Support a robust, end-to-end zero-trust security framework** that enhances productivity by connecting employees on any device, from any location, at any time, to any application
- **Enable dynamic and automated access policies** to secure any user, any device, any app, anywhere
- **Stop propagation of security incidents** using dynamic context, not location, for segmentation
- **Help ensure fast compliance** by applying security to thousands of locations from one interface
- **Automate threat responses** to quickly respond to threats and remediate incidents in less time

What it does

Security in depth

With the increased sophistication and number of network attacks, security is more important than ever. It's no longer possible to protect your most valuable assets with rudimentary, single-point security solutions. You need security in depth that's tightly integrated with your network infrastructure.

Think of the journey network traffic takes from the edge to the asset. Your security solution needs to be active at each of these touchpoints. You need advanced firewalls, ASA secure internet gateways, Umbrella SIG and intrusion prevention at the access points Adaptive iPS to protect the edges. You need to continually monitor software and OS versions PSIRT to patch any security vulnerabilities. You need to continually monitor your traffic—even when it's encrypted—to identify and contain breaches and malware. And all your security solutions need to be powered by the industry's leading threat intelligence Talos.

Zero-trust security

As networks have become more distributed, zero-trust security principles have become the security framework of choice. This approach is built on the concept that no device—from user laptops and smartphones to IoT devices and smart buildings—can be implicitly trusted based on a single, static identifier. Trust must be verified and continually monitored.

This approach is built on three principles. First, you need to identify and verify every device when it connects to your network—either through multifactor authentication Duo or AI-enabled endpoint analytics SD-Access. This is especially necessary for IoT devices, which must be compared with the key attributes of known devices and grouped with similar devices.

Second, you must be able to define and enforce the least privilege access for each of the identified devices ISE. Where can they connect, and what can they do? Network segmentation is then established to enforce these policies and minimize the lateral movement of threats.

And finally, you need to continually monitor and analyze your network traffic to stay atop intrusions and vulnerabilities. Secure Network Analytics. This is why it is so important to have the tight network and security integration that's possible through Cisco. Our network and security solutions share common telemetry and enforcement mechanisms, so when a device starts to exhibit out-of-policy behavior, it can automatically be quarantined. This approach can be very effective in controlling ransomware attacks. When ransomware tries to move laterally throughout an organization, Cisco network and security solutions identify the out-of-policy traffic, block access, and quarantine the device until it can be remediated.

Learn more

Too often, companies must choose between a robust security solution or an easy-to-access and reliable network. With Cisco Enterprise Network Security, you get both, with solutions that work better together. For more information, visit the Enterprise Network Security page. Or talk with your Cisco Sales representative.